Nanjing Univ. J. Natur. Sci. 37(2001), no. 4, 473–476.

A NOTE ON THE ERDÖS–GINZBURG–ZIV THEOREM

Jian-Xin Liu and Zhi-Wei Sun

Department of Mathematics, Nanjing University
Nanjing 210093, P. R. China

Abstract. Let G be an additive abelian group of order n, and $S = \{a_i\}_{i=1}^{2n-1}$ a sequence of $2n-1$ elements in G. For $a \in G$ let $r(S,a)$ denote the number of ways we can write a as the sum of n terms of S. If G is a subgroup of the additive group of F, where F is a field of prime characteristic p, then we have $r(S,0) \equiv 1 \pmod p$, and $r(S,a) \equiv 0 \pmod p$ for $a \in G \setminus \{0\}$. This extends W. D. Gao's recent work [2] on a theorem of Erdös, Ginzburg and Ziv.

Keywords: combinatorial number theory, abelian group, field of characteristic p.

0. Introduction

Let G be an additive abelian group of order n, and $S = \{a_i\}_{i=1}^{2n-1}$ a sequence of $2n-1$ elements of G. Set

$$r(S,a) = \left|\left\{ I \subseteq \{1,2,\cdots,2n-1\} : |I| = n \ \&\ \sum_{i\in I} a_i = a \right\}\right| \tag{1}$$

for $a \in G$. A famous theorem of Erdös, Ginzburg and Ziv [1] asserts that $r(S,0) \geqslant 1$. When $n = p$ is a prime, Gao [2] proved that

$$r(S,a) \equiv \begin{cases} 0 \pmod p & \text{if } a \neq 0, \\ 1 \pmod p & \text{otherwise.} \end{cases} \tag{2}$$

In this paper, we aim to extend Gao's result. Our main result is as follows:

Theorem. *Let F be a field of characteristic p and G be a subgroup of the additive group of F with $|G| = n$. Let $S = \{a_i\}_{i=1}^{2n-1}$ a sequence of $2n-1$ elements of G. Then (2) holds for all $a \in G$.*

This will be shown in the next section.

The research is supported by the Teaching and Research Award Program for Outstanding Young Teachers in Higher Education Institutions of MOE, and the National Natural Science Foundation of P. R. China (19971038).

Corollary. *Let F a finite field with $q = p^h$ elements where p is a prime and h is a positive integer. Then for any $a_1, a_2, \cdots, a_{2q-1} \in F$ we have*

$$\left|\left\{I \subseteq \{1,2,\cdots,2q-1\} : |I| = q \ \&\ \sum_{i\in I} a_i = 0\right\}\right| \equiv 1 \pmod p. \tag{3}$$

Proof. As F is of characteristic p, we can apply the theorem with $G = F$.

Throughout this paper, we think that an empty product takes the value 1 while an empty sum takes 0.

1. Proof of the Theorem

At first we give a lemma.

Lemma. *Let $n = p^h$ where p is a prime and h is a nonnegative integer. Then*

$$\binom{2n-1}{n} \equiv 1 \pmod p \tag{4}$$

and

$$\binom{2n-1-k}{n-1} \equiv 0 \pmod p \quad \text{for } k = 1,2,\cdots,n-1. \tag{5}$$

Proof. The case $h = 0$ is trivial, below we assume $h \geqslant 1$. Let $k \in \{0,1,\cdots,n-1\}$. Since $0 \leqslant n-1-k < n = p^h$, we can write $n-1-k$ in the form $\sum_{i=0}^{h-1} k_i p^i$, where $k_i \in \{0,1,\cdots,p-1\}$. Thus

$$\binom{2n-1-k}{n-1} = \binom{1p^h + k_{h-1}p^{h-1} + \cdots + k_0 p^0}{0p^h + (p-1)p^{h-1} + \cdots + (p-1)p^0}.$$

By a well-known theorem of E. Lucas (see Section 1 of Granville [3]),

$$\binom{2n-1-k}{n-1} \equiv \binom{1}{0}\binom{k_{h-1}}{p-1}\cdots\binom{k_0}{p-1} \pmod p.$$

If $k = 0$, then $k_0 = \cdots = k_{h-1} = p-1$ and hence

$$\binom{2n-1-k}{n-1} \equiv 1 \pmod p.$$

When $0 < k < n$, clearly $k_i < p-1$ for some $0 \leqslant i \leqslant h-1$ and hence

$$\binom{2n-1-k}{n-1} \equiv 0 \pmod p.$$

We are done. □

Proof of the Theorem. Suppose that $F \supseteq G$ is a field of characteristic p where p is a prime. If a prime q divides $n = |G|$, then by Cauchy's theorem in group theory (cf. Theorem 5.11 of Rose [4]), G has an element x of order q, thus $qx = 0$ and hence $p|q$ (i.e. $p = q$), since x is nonzero and p is the characteristic of F. This indicates that $n = p^h$ for some nonnegative integer h.

Let m be any nonnegative integer less then n. With the help of the multinomial theorem,

$$\begin{aligned}
\sum_{a\in G} r(S,a)a^m &= \sum_{\substack{J\subseteq\{1,\cdots,2n-1\}\\ |J|=n}} \Big(\sum_{j\in J} a_j\Big)^m \\
&= \sum_{\substack{I\subseteq\{1,\cdots,2n-1\}\\ |I|\leqslant n}} \sum_{\substack{I\subseteq J\subseteq\{1,\cdots,2n-1\}\\ |J|=n}} \sum_{\substack{m_i\geqslant 1 \text{ for } i\in I\\ m_j=0 \text{ for } j\in J\setminus I\\ \sum_{j\in J} m_j=m}} \frac{m!}{\prod_{j\in J}(m_j!)} \prod_{j\in J} a_j^{m_j} \\
&= \sum_{\substack{I\subseteq\{1,\cdots,2n-1\}\\ |I|\leqslant n}} \binom{2n-1-|I|}{n-|I|} \sum_{\substack{m_i\geqslant 1 \text{ for } i\in I\\ |I|\leqslant\sum_{i\in I} m_i=m}} \frac{m!}{\prod_{i\in I}(m_i!)} \prod_{i\in I} a_i^{m_i} \\
&= \sum_{\substack{I\subseteq\{1,\cdots,2n-1\}\\ |I|\leqslant n-1}} \binom{2n-1-|I|}{n-1} \sum_{\substack{m_i\geqslant 1 \text{ if } i\in I\\ \sum_{i\in I} m_i=m}} \frac{m!}{\prod_{i\in I}(m_i!)} \prod_{i\in I} a_i^{m_i}.
\end{aligned}$$

Applying the Lemma and noting that F is of characteristic p, we then obtain that

$$\sum_{a\in G} r(S,a)a^m = \sum_{\substack{m_i\geqslant 1 \text{ if } i\in\emptyset\\ 0=\sum_{i\in\emptyset} m_i=m}} \frac{m!}{\prod_{i\in\emptyset}(m_i!)} \prod_{i\in\emptyset} a_i^{m_i} = \begin{cases} 1 & \text{if } m=0,\\ 0 & \text{otherwise.}\end{cases}$$

Let $g_0 = 0$ and write $G \setminus \{0\} = \{g_1, \cdots, g_{n-1}\}$. Consider the following system of n linear equations:

$$\begin{cases} \sum_{j=0}^{n-1} g_j^0 x_j = 1 \\ \sum_{j=0}^{n-1} g_j^1 x_j = 0 \\ \cdots\cdots\cdots\cdots \\ \sum_{j=0}^{n-1} g_j^{n-1} x_j = 0. \end{cases} \tag{6}$$

Its determinant of coefficients is

$$\begin{aligned} D=&\begin{vmatrix} 1 & 1 & \cdots & 1 \\ 0 & g_1 & \cdots & g_{n-1} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & g_1^{n-1} & \cdots & g_{n-1}^{n-1} \end{vmatrix} \\ =&\begin{vmatrix} g_1 & \cdots & g_{n-1} \\ \cdots & \cdots & \cdots \\ g_1^{n-1} & \cdots & g_{n-1}^{n-1} \end{vmatrix} \\ =&g_1\cdots g_{n-1}\prod_{1\leqslant s<t<n}(g_t-g_s)\neq 0. \ \text{(Vandermonde)} \end{aligned}$$

So (6) has a unique solution. By the last paragraph, if $x_j = r(S, g_j)1$ for $j = 0, \cdots, n-1$, then (6) holds. On the other hand, evidently (6) has the solution $x_0 = 1$ and $x_1 = \cdots = x_{n-1} = 0$. As F is of characteristic p, $r(S, 0) = r(S, g_0) \equiv 1 \pmod p$ and $r(S, g_j) \equiv 0 \pmod p$ for $j = 1, \cdots, n-1$. This concludes the proof. □

References

1. Erdös P., Ginzburg A. and Ziv. A. *Theorem in the additive number theory* [J]. Bull. Research Council Israel, 1961, 10: 41–43.
2. Gao Weidong. *Two addition theorem on groups of prime order* [J]. J. Number Theory, 1996, 56: 211–213.
3. Granville. A. *Arithmetic properties of binomial coefficients.I. Binomial coefficients modulo prime powers* [C]. In: Organic mathematics (Burnady, BC, 1995), CMS Conf. Proc. 20, Amer. Math. Soc., Providence, RI, 1997: 253–276.
4. Rose, J. S. *A Course on Group Theory* [M]. Cambridge Univ. Press, 1978.